DOCKET FILE COPY ORIGINAL

January 19, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RECEIVED
JAN 26 1994
FCC - MAIL ROOM

RE: CC Docket 93-292

Dear Mr. Canton:

I was thrilled to read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As the Telecommunications Manager for the City of Provo, a Utah community of 120,000, I am encouraged by the proposed rulemaking. Even though we have taken each and every protective step recommended by the IXC's and CPE vendors, we still experienced toll fraud. I have sadly learned that it is impossible to secure any system from toll fraud.

I firmly believe that PBX owners should not be responsible for 100% of the toll fraud, since we don't have 100% control. Our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided by IXCs, LECs, and CPEs. The law should reflect that.

It is preposterous to think that the IXCs, LECs and CPEs have absolutely no legal obligations to even warn customers. It is galling to know, that these service and equipment providers consistently receive payment for the fraudulent calls made through equipment belonging to helpless PBX owners, and in many cases -- full payment. Where is their incentive to stop fraud? They appear to be much more concerned with limiting their liability.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs sell equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later. It is vital that the FCC establish a standard for caller identification and require the IXCs and LECs to pass this information. This would simplify both the identification and prosecution of hackers.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to

No. of Copies rec'd 0+1
List ABCDE

preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, toll fraud, when it did occur, could be limited to hours instead of days. The FCC should also consider requiring the LECs to offer monitoring services similar to the IXCs, as hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers.

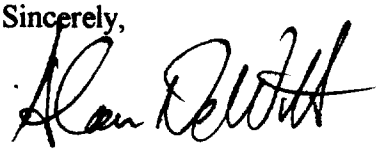
I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXCs and LECs to offer detection and prevention programs and education services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause. The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when hackers state, they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the $5 billion problem it is today. We must develop legislation that both clearly defines and penalizes this criminal activity and gives law enforcement the means to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am sure that if we all work together we can make a positive impact on this terrible problem.

Sincerely,



Alan L. DeWitt
Provo City Corporation
Facility Services Division

STATE OF CONNECTICUT
DEPARTMENT OF TRANSPORTATION

24 WOLCOTT HILL ROAD, P.O. BOX A
WETHERSFIELD, CONNECTICUT 06129-0801
Phone:

January 10, 1993

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXCs.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the of the toll fraud risks associated with features of the CPE, and the IXCs and LECs to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the $5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

Dolores E. Zukauskas

Dolores E. Zukauskas
Systems Coordinator
Bradley International Airport

Morris Communications Corporation

P.O. BOX 936 • AUGUSTA, GEORGIA 30903-0936

LOWELL R. DORN
Director of
Morris Information Services

January 10, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposal Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day. As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXCs.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the of the toll fraud risks associated with features of the CPE, and the IXCs and LECs to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the $5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

Lowell Dorn

Lowell R. Dorn

LRD/bw

Ball State University

Business Affairs
Telephone and Postal Services

January 20, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

Dear Mr. Canton:

As a telecommunication professional I am interested in the swift implementation of CC Docket no. 93-292.

Fraud control is and should be a shared responsibility among PBX owners and the IXC's, LEC's and CPE vendors.

Monitoring of calling activity by the IXC's should be standard operating procedure.

NPRM seems fair - it should clearly define the responsibilities of the parties.

I believe you are aware of the financial impact of toll fraud and ask that you help us all by pushing for the necessary reform regulations.

Sincerely,

Joseph P. Nial, Director
Telephone Services

JPN:rb

317-285-8417 Muncie, Indiana 47306-0775

ARTHUR ANDERSEN & Co SC

ARTHUR ANDERSEN | ANDERSEN CONSULTING

DOCKET FILE COPY ORIGINAL

January 14, 1994

One North State Street
Chicago IL 60602-3300
312 580 0069

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC. 20554

Re: CC Docket 93-292

RECEIVED

FCC - MAIL ROOM

Dear Mr. Canton:

It was with great interest that I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for supporting telecommunications systems in a firm with global presence, I am encouraged by your initiative to investigate and address the important issue of toll fraud.

Security is very important to us. We work diligently with equipment suppliers and carriers to insure that our systems have been installed and are maintained with all recommended security measures in place. In our experience, equipment suppliers and their technicians' knowledge of toll fraud risks and associated security measures vary greatly. The variance between vendors is understandable, but the variance within a single organization is not. The amount of attention paid to security aspects of the system is determined solely by the expertise of the specific installation or maintenance team. Some guidelines or standardization in this area would benefit all concerned parties.

It has been our experience that IXC monitoring of our lines has been hit or miss. We have been notified by one carrier several times of suspect usage and been able to halt fraud in progress quite quickly. On another occasion, notification was not made even though their systems flagged the unusual calling patterns. Another carrier wouldn't provide any call detail before the normal invoicing date or monitor usage on a real-time basis. This carrier assured us that we had experienced only a small amount of fraud during a weekend; then sent an invoice for 4000% more. A large number of our lines are dedicated ones which the IXCs monitor on a fairly regular basis. When calls are placed via the dial 1 carrier or using carrier access codes, there appears to be little, if any monitoring on the part of the IXC or the LEC.

Toll fraud is an illegal, fraudulent theft of service. Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the $5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Very truly yours,

Joan A. Johnstone

Joan A. Johnstone

Copies to:
Mr. Wayne W. Davidson, Chicago-69W
Ms. Teana P. Wright, Chicago-69W

No. of Copies rec'd 0+4
List ABCDE